MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 27 | Issue 3 Article 10

2001

E-commerce Privacy and the Black Hole of Cyberspace

Stephen R. Bergerson

E-COMMERCE PRIVACY AND THE BLACK HOLE OF CYBERSPACE

Stephen R. Bergerson†

I. INTRODUCTION

This article examines the unprecedented ability of online technology to discreetly gather personal information, where the information goes and how it is used. This article also discusses whether these practices constitute invasion of privacy under existing laws and if not, whether and to what extent laws might change to protect consumers from such practices. Finally, this article chronicles how the Federal Trade Commission and Congress have reacted to (and sometimes influenced) consumers' evolving views

† The author wishes to acknowledge the valuable research assistance of Jim Mayer, a second-year student at William Mitchell College of Law.

of online privacy, identifies the likely role of industry self-regulation and explains how international laws are influencing America's online privacy policy debate.

II. THE GALVANIZATION OF PRIVACY CONCERNS

While privacy concerns predate the personal computer, the advent of e-commerce has heightened consumers' concerns and intensified their distrust of information gatherers. The twentieth century's last decade witnessed a sea change in marketers' ability to electronically collect and compile personal information and a corresponding surge in the public's privacy angst. While the new technology increases marketers' ability to put more targeted, relevant and useful product information in consumers' hands, consumers wonder whether the privacy tradeoff is a fair one.

They now know that unseen databases burst with details about their habits, hobbies and home life—the fuel on which the Information Age runs. The debate over the risk and benefits of these changes has reached an intensity that has pushed it to the brink of congressional intervention.

A. *Initial Privacy Concerns*

Justice Louis Brandeis identified an individual's constitutional right to privacy as early as 1890.[1] Ever since, courts have used the U.S. Constitution to protect individual privacy from governmental intrusion[2] and state tort laws to protect against private intrusions.[3]

Privacy *legislation* appeared much later, first restricting government, then business intrusions.[4] Both judicial opinions and legislation, then, have influenced and reflected Americans' notions of privacy over time.

In the meantime, pollsters became interested in the public's views on the subject. In 1970, Harris Polls found that 33% of consumers expressed an overall concern about privacy. By 1993, that number had soared to 83%, and 71% of consumers felt they had lost all control over how their personally-identifying information was used. Seventy-nine percent said that a modern re-write of the

1. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
2. U.S. CONST. amend. I, III, IV, IX, XIV; *infra* Part III.A.
3. *Infra* Part III.B.
4. *Infra* Part III.C.

Declaration of Independence should add "privacy" to the fundamental list of "life, liberty and the pursuit of happiness."

While consumers have always been skeptical of governmental privacy intrusions, their concern has now shifted to direct marketers, especially online businesses. In a 1993 Harris Poll, 64% said that their level of trust in the way direct marketers handle information was "low." The San Diego Center for Public Interest Law's "Privacy Rights Hotline" took calls from 11,402 California residents in its first year. Sixty-four percent of them expressed concern about direct marketing in particular. By 1999, 92% of Americans were concerned about business' online misuse of personal information.[5]

One of Harris Poll's first surveys in the new millennium found that nearly half of those polled were "very concerned" that inaccurate information gathered from them could be used to deny them credit or insurance, or to defraud them.[6] A substantial minority were "very concerned" that inaccurate information could prevent them from getting a job (36%) or be used to embarrass them (28%).

The dissemination of *accurate* information scares people nearly as much. Many Americans are "very concerned" about accurate information being used to defraud them (30%) or to prevent their getting insurance (29%), credit or a job (27%).

More recent statistics are even more attention-getting: 57% of Americans surveyed in March, 2000 wanted federal laws regulating the collection and use of personal information on the Internet.[7] In October, a survey commissioned by the National Consumers League showed that 56% of Americans say they are more concerned about losing personal privacy than about health care, crime or taxes. And nearly two-thirds of Internet users and more than three-fourths of non-users believe that people who go online put their privacy at risk, according to the UCLA Internet Report, also released in October. These feelings have not gone unnoticed by politicians; there are currently over fifty privacy bills pending in

5. Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, PRIVACY AND AM. BUS., Nov. 1999, at 11 (quoting Dorothy A. Hertzel, Note, *Don't Talk To Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429, 432 (2000)).

6. The Harris Poll #1 (Jan. 5, 2000).

7. Kent Hoover, *Consumers Push For Online Privacy Laws*, MPLS./ST. PAUL CITY BUS., May 12, 2000, at 12.

Congress.[8]

While industry has argued for the chance to "regulate" itself from the start, the public and government have both decided that the industry moved too slowly and unconvincingly as privacy fears rose among the populace. Fifty-nine percent of Internet users surveyed "do not trust companies' ability or intention to keep personal information confidential, regardless of what their privacy policies say."[9]

These fears escalated as consumers became more aware of the increased sophistication of data collection techniques and of the growing prevalence of e-commerce. In fact, "76% of consumers who are generally not concerned about the misuse of personal information are afraid of privacy intrusions on the Internet."[10] The intimate nature, immediacy, interactivity and popularity of online transactions have combined to intensify people's natural inclination to protect their privacy.

B. The E-Commerce Explosion

The electronic marketplace has grown at a previously (and still) unimaginable pace since it emerged in the mid-1990's.[11] Online sales tripled from $3 billion in 1997 to $9 billion in 1998.[12] Some estimates put 1999 online sales at $33 billion and project 2000 sales at a staggering $61 billion.[13]

Online advertising has risen at a similarly meteoric rate: spending rose sharply from $1.9 billion in 1998 to $4.6 billion in 1999 and has increased more than ten-fold since 1996.[14] In inflation-adjusted dollars, Internet advertising spending growth is significantly outpacing the comparable spending during television and radio's early years.[15]

---

8. *Id.*

9. *Id.*

10. FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress* (May 2000) (citing Louis Harris & Associates, Inc., *IBM Multi-National Consumer Privacy Survey*, Oct. 1999, at 73).

11. *Id.* at i.

12. *Retail E-Commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion,* U.S. Dep't. of Comm. News (Census Bureau), Mar. 2, 2000.

13. *Online Retailing in North America Reached $33.1 Billion in 1999 and is Projected to Top $61 Billion in 2000,* SHOP. ORG NEWS (Apr. 17, 2000), *available at* http://www. shop.org/nr/00/041700.html.

14. FTC, *supra* note 10, at 2.

15. *Internet Advertising Burearu, Internet Advertising Revenue Report: Executive Summary 1999 Third Quarter Results,* INTERNET ADVER. BUREAU, *available at*

Despite its phenomenal growth, e-commerce is still in its infancy. Today, the United States leads the world in both e-commerce activity and Internet access, with about 90 million Americans using the Internet on a regular basis.[16] However, the level of European Internet access will soon exceed that of the United States and Asia will have 80 million Internet users by 2003.[17] The number of Latin American Web users is expected to increase from 5 million to 19 million during that time.[18] In other words, nearly half of the globe's e-commerce will soon be attributable to other countries ... compared with thirty percent today.[19] The result? America's e-commerce companies will soon be influenced by foreign or foreign privacy rules, discussed in Section IV of this article.

C. *Consumer 'Profiling': Boon Or Bane?*

1. *The Marketer's Perspective*

Why does Internet data collection make marketers salivate? For years, marketers have used consumers' demographic information to more narrowly target and increase the efficiency and effectiveness of their marketing communications efforts.

New online technologies have created easier and even more efficient and effective ways to gather and use such information. As early as 1995, FTC Commissioner Christine Varney foresaw the Internet's potential, "In the area of data-gathering and use by online businesses, the new technology has made it possible not only to store personal information provided by consumers but also to track consumers' decisions as they move through online sites, whether or not they complete transactions."[20]

One new technology, called "cookies," enables web site owners to discretely capture information about their visitors' computers, browsing patterns and items purchased.[21] When consumers visit a

---

http://www.iab.net/news/content/ 3Q99exec.html.

16. *The Intelliquest Technology Panel, at* http://www.techpanel.com/news/index.asp.

17. James Heckman and Kathleen V. Schmidt, *International in Internet Closes U.S. Lead*, MKTG NEWS, Feb. 14, 2000, at 7.

18. *Id.*

19. *Id.*

20. FTC Commissioner Christine Varney, Remarks at the Privacy and American Business Conference (1995).

21. FTC, *supra* note 10, at n.53.

website, a "cookie" is attached to their hard drive which makes navigation there easier for future visits because the site is able to "recognize" them. However, cookies are mere appetizers for Internet marketers, who can also monitor and capture surfing behavior, frequency of consumer web site visits and amount of time per visit across the entire Internet, enabling them to create extremely detailed profiles of individual consumers.[22] Businesses use these identifiers to create, sell, rent or otherwise share customer profiles with other businesses for their respective commercial purposes.[23]

Although these so-called "passive" methods of data-collection yield "non-identifying" data, these methods can be easily combined with personally identifying information to create remarkably (and to many, frighteningly) detailed personal consumer profiles.[24]

This combined data allows marketers to target their promotional efforts only to those who are most likely to be interested in them. Conversely, consumers receive more interesting, relevant and useful information with less "junk." Even Commissioner Varney emphasized this benefit, albeit in an era before the FTC became more strident on privacy issues, pointing out that Internet marketing has provided consumers "a staggering array of information with which to make purchasing decisions."[25] If business expected consumers to enthusiastically embrace the tradeoff, they could not have been more wrong.

2. The Consumer's Perspective

Why does online shopping evoke such strong privacy concerns? Why does online data collection make consumers tremble? For years, consumers have unhesitatingly shared personal information with marketers through registration, warranty and order forms, surveys, contests, magazine subscriptions and loyalty programs. Stay-at-home interactive shopping is a big part of what makes e-commerce attractive to consumers. It also is what heightens their privacy concerns: they are more sensitive to privacy when in their own home, the most intimate of settings. Additionally, online information collection is not what people seeking to avoid

22. *Id.* at n.59.

23. Consumers can buy software to block sites who try to collect "cookies." *See* MERCHANT & GOULD, P.C., MINN. DEP'T. OF TRADE AND ECON. DEV., A LEGAL GUIDE TO THE INTERNET 94 (Aug. 1999).

24. *Id.* at 10.

25. *Infra* Part III.E.

crowds and cashiers expected—or wanted—to find online.[26] Finally, the Internet is still new, and surrounded by an aura of both intrigue and skepticism.

These electronic data gathering and consumer profiling practices and the consequent improvements in target marketing bring to mind the Restatement of Torts' definition of "intrusion upon seclusion." The definition states, "The invasion may be by physical intrusion .... It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires."[27]

Essentially, online technology allows businesses to 'peer over consumers' shoulders as consumers browse online from their own homes. A customer may not be troubled when a local bartender serves up their favorite beer before they even order it. However, imagine the same thing happening in a pub on the other side of the country: impressive—but disconcerting—service. Moreover, much of the information that can be assembled (such as health or financial status) is considerably more sensitive than their choice of beverage. It is now quite possible if you shop online.

Online information gathering technology "reduces the cost and increases the speed with which private information can be duplicated," and "the cost of performing these functions does not vary with distance; it is as cheap to perform from halfway around the world as it is from the next room."[28] Even more frightening, the information can be stored on a database platform that is potentially accessible to the entire Internet world and used for purposes other than that for which it was intended.[29] Marketers call it a miracle. Consumers call it "spooky."[30]

---

26. Perhaps the desire for anonymity reflects a larger societal shift in values: "In the days of the mom-and-pop grocery, the shopkeeper always knew what his regular customers would buy. But consumers have come to value the anonymity of shopping at the modern supermarket. If you have a $17.98-a-week Twinkies habit, nobody has to know (except, perhaps, your cardiologist)." *The Price of Privacy*, ADWEEK, Dec. 18, 1995.

27. RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1977).

28. HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY § 3.1 (Supp. 2000).

29. George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, J. PUB. POL'Y & MKTG., Spring 2000, at 1.

30. Carol Krol, *A Hot Marketing Concept is Running Smack into Big Concerns About the Extent of Company Usage of Personal Information: Consumers Reach the Boiling*

William Mitchell Law Review, Vol. 27, Iss. 3 [2001], Art. 10

Industry's recognition of and reaction to consumer concerns was slow and inadequate. The business community largely ignored America Online CEO Steve Case's warning that technological advances would be less important to the Internet economy's growth than public policy decisions. Industry's failure to seize the policy initiative has allowed others to take the lead in determining how e-commerce will do business in the twenty-first century.[31]

Government is now leading the privacy initiatives. Online privacy has become a political and policy juggernaut. Nearly every candidate for political office has "consumer privacy" on their lips.

III. PRIVACY PROTECTION

As previously indicated, the U.S. Constitution provides an opportunity for courts to conceptualize a right of privacy. Even though its provisions apply only to *government* actions, the Constitution is the context within which *all* privacy debates have since taken place.

Existing state tort laws have little potential to help protect online privacy, and have not yet been much used for that purpose. Consequently, state and federal *legislation* will have the most significant effect on online data gathering privacy issues. Industry self-regulation will play an important—but secondary—role. And consumers themselves will learn how to protect their own privacy by opting out of data collection, providing false online information and increasingly exercising both market and political influence on privacy practices and policies.

A. *Federal Constitution*

In a famous passage in *Griswold v. Connecticut*,[32] Justice Douglas recognized that "[t]he specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[33] He concluded that "emanations" from the First, Second, Fourth, Fifth and Ninth Amendments cre-

---

Point Over Privacy Issues, ADVER. AGE, Mar. 29, 1999, at 22 (quoting Jason Catlett, President of Junkbusters Corporation who stated: "Some targeted offers are so accurate that they spook the consumer. Marketers talk about having a relationship with the consumer; if that's not something the consumer wants, then it's a liability.")

31. *Id.*

32. 381 U.S. 479 (1965).

33. *Id.* at 484.

ated a "zone of privacy" in which individuals are protected from government interference.[34] But since constitutional and legislative protections have historically not addressed *private* intrusions, there are no statutes for consumers to look to now that they have realized the Internet's privacy implications.[35]

B. State Tort Law

Virtually all states recognize four forms of invasion of privacy: 1) intrusion upon seclusion; 2) commercial appropriation of a person's name or likeness; 3) unreasonable publication of private facts; and 4) placing a person in a false public light.[36] All were established long before the dawn of the Information Age as we know it[37] and courts have been unwilling to extend these theories to online information gathering practices or to recognize a common law right to information privacy.[38]

Of the four, intrusion upon seclusion seems the most applicable, although even it requires a stretch. Much online data is voluntarily provided, even though consumers may subsequently object to its *use*. Even when consumers are unaware of the data collection, the reach of this theory is limited by the "highly offensive to a reasonable person" requirement—although the day may come when courts will be willing to so classify the unauthorized commercial use of such data.[39]

Since this tort has historically been applied to physical intrusions (with the exception of phone tapping)[40] courts seem unlikely to expand the concept much beyond traditional trespass anytime soon.[41]

The tort of appropriation of name and likeness protects "the interest of the individual in the exclusive (commercial) use of his own identity."[42] It seems inapplicable to online information gather-

34. *Id.* State governments are kept out of this zone of privacy by the Fourteenth Amendment. *Id.* at 487-88.

35. *Infra* Part III.C.

36. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

37. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

38. For a comprehensive discussion of technology and state and federal privacy law, see Sandra Byrd Petersen, Note, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163 (1995).

39. RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1977).

40. *Id.* at § 652B cmt. b.

41. Prosser, *supra* note 37, at 392.

42. RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977).

William Mitchell Law Review, Vol. 27, Iss. 3 [2001], Art. 10

ing and use, since cases have traditionally dealt with instances in which a person's name or likeness have been appropriated for advertising purposes.

The third form of invasion, unreasonable publication of private facts, is of little use because it requires that "[T]he matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[43] Even if information collected online is sold to other entities, it seems unlikely to become a matter of "public knowledge" as the phrase has been used in privacy decisions.

Finally, the "false light" form of invasion of privacy seems wholly inapplicable, because it requires that the information be false, and that "the actor had knowledge of, or acted in reckless disregard as to the falsity of the publicized matter."[44] The value of personal information, of course, is derived in large part from its *accuracy*, not its falsity, and to the extent that it is false, it is unlikely to have been shared by the person who later complains.

The leading privacy tort case is *Shibley v. Time, Inc.*,[45] in which an Ohio Court of Appeals held that the sale of a mailing list does not give rise to a privacy cause of action. Some courts have generally adhered to *Shibley* ever since. Others argue that *Shibley* should be revisited in light of changed circumstances.[46]

Since data collection methods have improved in sophistication, the law should distinguish between simple mailing lists, such as *Time*'s subscriber list in *Shibley*, and targeted mailing lists. This suggested approach has not been reflected in any reported court decisions.

For these reasons, some argue for the creation of a new statutory cause of action for commercial dissemination of private facts.[47]

C. *Federal Legislation*

Various state statutes address information privacy issues in specific and especially sensitive areas such as health and financial information. Some states are fearful that businesses will choose not

43. *Id.* § 652D cmt. a.
44. *Id.* § 652E (b).
45. 341 N.E.2d 337 (Ohio Ct. App. 1975).
46. Stephen P. Durchslag, *Privacy and Mailing Lists*, PROMO, Jan. 1997, at 92.
47. *See* Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987).

to conduct business there if they impose restrictive regulatory regimes, as demonstrated by the unanticipated effects of the Gramm-Leach-Bliley Act, discussed later in this section. State regulation also raises problems of personal jurisdiction and choice of law (which are beyond the scope of this article).

For these and other reasons discussed in this article, Congress is now addressing e-commerce privacy issues. In fact, consumer privacy bills are at the height of congressional fashion this election year.[48] The proliferation of privacy bills is a product of political posturing, increased dissatisfaction with industry's self-regulatory efforts and the growing consumer awareness and concerns previously discussed.

1. *Federal Privacy Statutes Before 1998*

The existing federal statutes that protect consumer privacy from *private* intrusions are the result of a reactionary and piecemeal approach. In 1970, Congress enacted the Fair Credit Reporting Act ("FCRA"),[49] aimed at the credit reporting industry. The Act addressed "respect for the consumer's right to privacy"[50] by requiring reporting agencies to provide credit information only to those whom they believe will "use the information in connection with a credit transaction involving the consumer ... or otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer" or for the purposes of employment, insurance or determining eligibility for government benefits.[51]

While the FCRA's protection is limited by the vagueness of its own terms, particularly "legitimate business need", consumer protection was nonetheless enhanced by giving consumers the right to correct errors in their credit reports. While the FCRA has very limited applicability to e-commerce, it evidenced congressional interest in the collection, dissemination or disclosure of personal information.

In 1980, Congress took another specific but significant step when it passed the Electronic Funds Transfer Act ("EFTA").[52]

48. Kent Hoover, *Online Privacy Advocates Push For Additional Legislation*, CITY BUS., May 8, 2000, at 12.
49. 15 U.S.C. § 1681(a)-(t) (1988).
50. *Id.* § 1681(a)(4).
51. *Id.* at (b)(3).
52. 15 U.S.C. § 1693.

While the EFTA only applies to financial institutions, it is significant because it requires financial institutions to *notify* customers before disclosing their records to third parties. In 1984, Congress enacted a similar measure addressed to cable companies, prohibiting disclosure of customer information without *customer consent.*[53] The concepts of *notice* and consumer *consent* have since become core issues in the online privacy debate.

Similarly, the 1998 Video Privacy Protection Act prohibits *non-consensual* disclosure of customers' video rental choices.[54] The Act was passed after video rental records of a well-known jurist were made available to the media during Supreme Court confirmation hearings.[55]

Congress took another step in 1993, passing the Driver's Privacy Protection Act ("DPPA"),[56] which restricts the ability of state government agencies to sell driver's license records. While the DPPA applies only to state government agencies, it also addresses issues now at the forefront in the online privacy debate. It was passed in the aftermath of the murder of a well-known actress, whose murderer obtained her address from motor vehicle registration records.[57] The danger that the DPPA seeks to remedy is highly relevant to the online gathering of information (in 1998, the FTC reported that 62.9% of Web sites collected postal addresses).[58]

Congress' reactionary and piecemeal approach to protecting privacy rights has many clamoring for broader regulation. Sandra Byrd Petersen argued in 1995 that:

> Legislative responses to the Bork confirmation hearings and the Schaeffer murder are unfortunately typical. When evidence of a large problem arises, Congress commonly reacts with the quickest possible remedy. Therefore, instead of taking the opportunity to examine the entire issue of information privacy, Congress has looked only to the problem immediately facing it. This has resulted in solutions that are far too shortsighted and reactionary.[59]

Even when Congress tries, its legislation can have unantici-

53. 47 U.S.C. § 551 (1994).
54. 18 U.S.C. §§ 2710-2711 (1998).
55. Petersen, *supra* note 38, at 182.
56. 18 U.S.C. § 2721 (1994).
57. Petersen, *supra* note 38.
58. Mary J. Culnan, *Protecting Privacy Online: Is Self-regulation Working?*, J. PUB. POL'Y & MKTG., Spring 2000, at 23.
59. *Id.*

pated effects. The 1999 Gramm-Leach-Bliley Act was designed to improve privacy protection in the insurance, banking and securities industries, but has actually diminished it. The Act restricts the kind of information that financial institutions can share with industry affiliates, and requires them to notify customers before sharing personal information. But states which had already adopted more stringent standards "may find themselves at a competitive disadvantage compared with those that choose to comply minimally with federal law."[60]

Congress, at the urging of consumer groups and the FTC, may have learned a lesson from the Gramm-Leach-Bliley effect and now be taking Ms. Petersen's advice. In 1998, it passed the Children's Online Privacy Protection Act[61] and its current debate over numerous consumer privacy bills reflects what has become a priority to enact more comprehensive consumer privacy legislation. Congress' transformation from "hands-off" to "full speed ahead" has been substantially influenced by the FTC's evolving policy position.

2. Administration And FTC Policies

In June, 1995, the Clinton administration's National Information Infrastructure Task Force ("NIITF") issued "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information," which set forth "principles" to guide a privacy discussion that would focus on the "shared responsibility" of consumers, government and business for openness, accountability and consumer education.[62] The three "fundamental concerns" surrounding the online acquisition, disclosure and use of personal information were that:[63]

(1) an individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured;

(2) personal information should not be inappropriately altered or destroyed; and

(3) personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and

60. Adam Wasch, *Gramm-Leach-Bliley-Act May Cause Loss of Insurance Privacy Protection for Some*, ELEC. COM. AND L. REP. (2000).

61. 15 U.S.C. § 6501 (1998).

62. SEC. 13 COUNCIL OF BETTER BUS. BUREAUS, INC., DO'S AND DON'TS IN ADVERTISING, § 1, 701 (1996).

63. *Id.* at 702.

used.

The Privacy Principles "emphasize(d) *disclosure*, rather than prohibition of the use of personal information."[64] They "impose(d) significant new obligations on businesses to disclose relevant information about why the information was being collected, what the information would be used for, what steps would be taken to protect that information, the consequences of providing or withholding information and any rights of redress consumers may have."[65] The emphasis on disclosure, coupled with consumer responsibility, or "empowerment," popularized the notion of giving consumers an ability to "*opt out*", which remains a major point of contention in the privacy debate.[66]

The evolution of the FTC's views merit a closer look because they have influenced the privacy debate more than any other regulatory agency and because the FTC has become the leading voice in the debate over online privacy issues. The FTC quickly followed the administration's lead and undertook a "Privacy Initiative," the goal of which was to "avoid cumbersome regulation by facilitating the development of a set of *voluntary* principles to govern the use of consumer information in on-line transactions."[67] The Initiative was a self-described experiment in "conversational government." Like the NIITF's Principles, the FTC emphasized industry's role in *informing* consumers about data collection practices.

While important policy declarations, neither the NIITF's Principles nor the FTC's Initiative created enforceable, substantive rights. In fact, the FTC has no regulatory authority over online practices unless they are within its traditional "unfair" or "deceptive" trade practices jurisdiction.

At that time, the fear of stifling e-commerce with "cumbersome regulation" was a persuasive argument against privacy legislation and industry voluntary self-regulation was the preferred solution. The eventual loss of enthusiasm for the concept of self-regulation was driven in part by industry's inability to be proactive in seizing the opportunity to show that it could keep its own house in order and in part by the effectiveness of the disclosure principle: as people learned about the extent to which personal information was being collected and used, businesses learned that an *educated* con-

64. *Id.* at 704.
65. *Id.* at 703.
66. *Infra* Part V.
67. COUNCIL OF BETTER BUS. BUREAUS, INC., *supra* note 62, at 704.

sumer is often an *angry* one.[68]

Thus, less than a year later, the FTC began to change the tone of its 'conversation.' In June, 1996, after an FTC cyberspace privacy hearing, FTC Chairman Robert Pitofsky urged industry to adopt voluntary codes and hinted at the consequences if industry didn't get its privacy act together.[69] In a tone that contrasted with the 'we're all in this together' tenor of the Privacy Initiative, Mr. Pitofsky stated: "We are not shying away from regulation, but what happens if [a Web site's communication] is not deceptive or unfair?"[70] While putting pressure on industry, Mr. Pitofsky may also have been gently suggesting that Congress extend FTC authority to specifically include online privacy. Industry self-regulation was falling out of favor.[71]

In 1998, the FTC further increased the pressure by issuing a stinging rebuke of industry's efforts and more directly appealing to Congress for expansive regulatory authority. It began in the narrow and controversial context of children's Web sites. Mr. Pitofsky cited an FTC study showing that of 1,200 marketer Web sites, 85% collected personal data while only 14% disclosed their information practices to consumers.[72] More troubling, 89% of children's sites collected such information but only 23% asked children to get parental permission before obtaining it.[73] Only 10% gave parents control over any information collected from children.[74]

Mr. Pitofsky sternly warned: "Right now, we would view self-regulation as not working, [and] we are not willing to wait [any longer] at all with regard to protecting children's information privacy ... [Congress] ought to act promptly."[75] It did, passing the

68. Krol, *supra* note 30, at 22.

69. Ira Teinowitz, *FTC Chairman Seeking Voluntary Web Rules; Worries About Access, Privacy Drive Push for New Standards on Marketer Sites*, ADVER. AGE, June 10, 1996, at 42. Mr. Teinowitz summarized the message that came out of the 1996 FTC hearing: "The World Wide Web's image as a Wild West of Marketing is about to get a fast roping-in thanks to new privacy-oriented industry codes and technological advances." *Id.*

70. *Id.*

71. To further protect consumers, the FTC discussed the availability of new technologies to allow consumers to avoid Web sites that did not meet privacy standards. *Id.*

72. Ira Teinowitz, *FTC Chief Asks Congress to Ensure Privacy on Web: Pitofsky Calls Voluntary Effort 'Disappointing'; Wants Parental Ok's Required*, ADVER. AGE, June 8, 1998, at 53.

73. *Id.*

74. *Id.*

75. *Id.*

Children's Online Protection Act ("COPPA") the same year.[76]

About the same time, the FTC began using its deceptive trade practices jurisdiction to challenge online data practices.[77] The first major case was brought against GeoCities,[78] a popular children's web site that offered personal home pages and email service. Its membership application forms requested both "mandatory" and "optional" information. Applicants were also asked to indicate whether they wished to receive specific "special offers" from advertisers.

According to the FTC, Geocities misrepresented that the personal information would be used only for the specific offers agreed to and that the "optional" information would not be shared with anyone. The FTC alleged that GeoCities disclosed the information to third parties who then made solicitations to which members had not agreed. The FTC further alleged that GeoCities had engaged in deceptive trade practices by collecting personally identifying information from children in contest and club application forms while misrepresenting that it operated the contests and maintained the information, when the contests and clubs were actually run by third parties who maintained the information.

GeoCities quickly settled the case by agreeing to post an online notice informing consumers of what information was being collected and what would be done with it. The notice told consumers how they could access and remove their personal information. Finally, GeoCities agreed to get parental consent before gathering any personal information from children twelve and under. The terms of the *GeoCities* settlement are remarkably similar to other federal legislation that has since been proposed.

Also in 1998, the FTC released the first of three Reports to Congress addressing online privacy. It laid out five "fair information practice principles" that were to guide industry self-regulation efforts: notice, choice, access, security and redress,[79] and it concluded that "an effective self-regulatory system had yet to emerge

76. *Infra* Part III.C.3.

77. For other instances of FTC enforcement actions, see FTC v. Reverseauction.com, Inc., FTC File No. 0023046 (D.D.C. Jan. 6, 2000) (settling charges involving the collection of personal data from a competitor site for the purpose of sending deceptive email messages); Liberty Financial Companies, Inc., FTC File No. 9823522 (May 6, 1999) (alleging misrepresentation that information collected from children would be maintained anonymously).

78. *In re* GeoCities, FTC File No. 9823015 (Aug. 13, 1998).

79. FTC, *Privacy Online: A Report to Congress,* at 7-11 (June 1998).

and that additional incentives were required in order to ensure that consumer privacy would be protected."[80] In congressional testimony in July, 1998, the FTC, while not taking a position on the need for legislation to protect *adults* online, did present a legislative model that Congress could consider if industry failed to develop and implement effective self-regulatory measures.[81]

Industry finally started to respond to the FTC's increasingly pointed warnings and, in its 1999 Report, the FTC noted that "online businesses are providing significantly more notice of their information practices than they were last year. In addition, several significant and promising self-regulatory programs–are underway."[82] The Report concluded that industry leaders should be commended for their "substantial effort and commitment to fair information practices" and that "legislation to address online privacy is not appropriate at this time."[83] The FTC also reaffirmed both its and the Clinton administration's position that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[84] Industry was being given another chance.

But industry's self-regulatory momentum stalled. A year later, the FTC's 2000 survey revealed that only 20% percent of Web sites had implemented the principles of notice, choice, access and security.[85] Only 41% of Web-sites posted 'opt out' information.[86]

While new self-regulatory "seal" programs (discussed later) were noted as "significant accomplishments," only "8% of heavily trafficked Web sites display(ed) a seal from one of them."[87] Citing industry's failure to meet "the meaningful broad-based privacy protections the Commission was seeking and that consumers want," the FTC concluded that, "industry efforts alone have not been sufficient to properly protect privacy rights."[88] The Report gave Congress the signal it needed to start the privacy legislation band-

80. FTC, *Self-Regulation and Privacy Online: A Report to Congress,* at 4 (July 1999).
81. *Id.*
82. *Id.* at 6.
83. *Id.* at 12.
84. *Id.* at 6.
85. FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress,* at 13 (May 2000).
86. *Id.* at 35.
87. *Id.*
88. *Id.*

wagon.

3. Congressional Response

As previously noted, Congress had already passed the Children's Online Privacy Protection Act in 1998 at the FTC's urging.[89] It provides: "An operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, may not collect personal information from a child in a manner that violates regulations prescribed by the FTC."[90]

The FTC's COPPA regulations require *notice* of what information is being collected and how it will be used.[91] They also require operators to get verifiable parental *consent* before collecting personal information[92] and require that parents be given the opportunity to *refuse* further retention of the information.[93] COPPA also contains a "safe harbor" provision, allowing operators to presumptively comply with COPPA by following "a set of self-regulatory guidelines, issued by representatives of the marketing or online industries or by other persons, if such guidelines are approved by the FTC."[94] FTC Rules implementing COPPA took effect April 21, 2000.[95]

About the same time, Senator John D. "Jay" Rockefeller, joined by nine other senators, introduced legislation that would allow Web sites to collect personal data only if consumer's expressly "opted in" (affirmatively indicated their willingness) to data collection.[96] The bill also proposed the creation of an "Online Privacy Office" within the FTC.

Other congressionally proposed bills were the Electronic Privacy Rights Act, which would require companies to obtain consent from consumers before collecting any personal data, and the Privacy Commission Act, which would establish a commission to study privacy issues. Senator John McCain introduced legislation that would require greater information practices disclosure by Web

89. *Supra* Part III.C.2.
90. 15 U.S.C. § 6502 (1998).
91. *Id.* § 1303(b)(1)(A)(i).
92. *Id.* at (ii).
93. *Id.* at (b)(1)(B); PERRITT, JR., *supra* note 28, at 35.
94. *Id.* § 1304 (1998).
95. 16 C.F.R. § 312 (2000).
96. *FTC Concludes Self-Regulation Not Enough To Protect Privacy, Recommends Legislation*, ELEC. COM. & L. REP. (May 2000).

sites, which he plans to advocate next term.[97]

With fifty privacy bills pending before Congress, and the Chair of the Senate Commerce Committee issuing warnings, the question is no longer *whether* online information practices will be legally regulated, but *to what extent.* If pervasive legislation is to be avoided, industry will need to quickly expand its self-regulatory efforts.

D. Industry Self-Regulation

Industry self-regulation, as distinguished from government regulation, is driven by industries' goals of treating consumers' fairly, promoting marketplace confidence and relieving government of the need to intervene. Typically, individual industries adopt principles and standards of practice to which its members are expected to voluntarily adhere.

Because of anti-trust constraints, industry cannot discipline or punish those who do not abide by these voluntary codes or guidelines. Consequently, industry is limited to using 'moral suasion' and implicit peer pressure to encourage compliance and its effectiveness varies from industry to industry and over time.

Self-regulation advocates advance a number of arguments as to why it is preferable to government regulation. Some argue that the "dynamic nature of Web site creation" makes regulatory enforcement impossible, leaving consumers with a false sense of security.[98] Others maintain that government intervention would suppress the growth of e-commerce, decrease competition, reduce customer choice and give older companies with established databases an unfair advantage.[99]

Privacy advocates wonder whether the same arguments don't apply to self-regulation, and whether it alone can effectively protect consumer privacy. IBM took a major self-regulatory step with its March, 1999 announcement that it would no longer advertise on Web sites which didn't clearly post their privacy policies.[100] At the

97. Jennifer Gilbert, *Ad Groups Hail Privacy Pact, Rivals Voice Fears; DoubleClick Rep. Calls Agreement 'Tough but Fair'*, ADVER. AGE, July 31, 2000, at 3.

98. Eve M. Caudhill & Patrick E. Murphy, *Consumer Online Privacy: Legal and Ethical Issues*, J. PUB. POL'Y & MKTG., Spring 2000, at 11.

99. *Id. See also* John R. Brandt, *What Price Privacy?*, INDUS. WK, May 4, 1999, at 4.

100. Jon G. Auerbach, *To Get IBM Ad, Sites Must Post Privacy Policies*, WALL ST. J., Mar. 31, 1999, at B1, B4.

time of the announcement, only thirty percent of the available Web sites clearly posted their privacy policies.[101]

While such individual business policies do contribute to online information protection and increase consumer confidence, they will not lead to uniform standards or eliminate consumer distrust, because a majority of Internet users "do not trust companies' ability or intention to keep personal information confidential, regardless of what their privacy policies say."[102]

One of industry's most far-reaching efforts has been "seal" programs, in which third parties "provide legitimacy and trustworthiness" to Web sites by allowing them to display a seal of approval if they comply with certain privacy requirements.[103]

The first seal program was TRUSTe, an industry initiative backed by AT&T, Oracle, Netscape and other industry leaders. Sites which follow the standards of notice, choice, access and security advocated by the Online Privacy Alliance, a coalition of industry groups,[104] can post the TRUSTe symbol. TRUSTe conducts periodic reviews of the site's privacy practices, verifies that they promptly remove personal information from databases upon consumers' requests and track changes in their privacy policies. TRUSTe also helps resolve consumer complaints and refers unresolved matters to the FTC.[105]

The Council of Better Business Bureaus ("CBBB") provides a similar service by allowing qualifying Web sites to post the BBB*OnLine* Privacy Seal. Applicants must maintain adequate privacy policies, submit to monitoring and review, and agree to a CBBB consumer dispute resolution process–the results of which are publicly reported. BBB*OnLine* also refers unresolved matters to federal agencies.[106]

In addition to these universally-available seal programs, more sector-specific programs have been recently created.[107] CPA WebTrust offers its seal to qualifying certified public accountants. The Interactive Digital Software Association ("IDSA") promulgated information practice guidelines in 1998. The Entertainment Soft-

101. Caudill & Murphy, *supra* note 98, at 11.
102. FTC, *supra* note 10.
103. Caudill & Murphy, *supra* note 98, at 11.
104. Federal Trade Commission, *supra* note 80, at 9-10. The OPA guidelines are similar to guidelines set forth by the FTC. *Id.*
105. *Id.* at 10.
106. *Id.*
107. *Id.* at 11.

ware Rating Board offers its seal to members who follow the IDSA guidelines and monitors compliance through audits. It also operates a consumer hotline to report violations, and provides alternative dispute resolution for consumer complaints.[108]

While useful privacy protection tools, seal programs do have limitations. Since they are voluntary, Web site operators can ignore them. Thus, while formerly optimistic about the progress of seal programs, the FTC reported this year that "[n]otwithstanding several years of industry and government effort, only 8% of heavily-trafficked Web sites display a seal from one of the self-regulatory seal programs." These limitations were part of the basis for the FTC's call for federal online privacy legislation. Nevertheless, "seal" programs will continue to be useful, especially when coupled with the concept of "safe harbor" provisions, examples of which are found in COPPA.

An FTC rule which implements COPPA provides that: "An operator will be deemed in compliance with the requirements of this part if the operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission."[109]

This rule also sets criteria for the approval of self-regulatory guidelines, which include a requirement that the guidelines implement COPPA's protections, contain an "effective and mandatory" system of independent compliance assessment, and offer effective incentives for compliance.[110] Companies which comply with an approved seal program are deemed to be in compliance with the government rule which incorporates it.

Similarly, the U.S. Department of Commerce recently reached a landmark agreement with the European Union, designed to facilitate international e-commerce in the face of existing and much more restrictive European privacy laws, as discussed later. It presumes legal compliance by U.S. companies doing business in Europe when they adhere to government-approved safe harbor privacy principles developed by the private sector.[111]

---

108. *Id.*

109. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.10(a) (2000).

110. *Id.* § 312.10(b).

111. PERRITT, JR., *supra* note 28, at 39-44 (citing U.S. Department of Commerce, *International Safe Harbor Privacy Principles* (Apr. 19, 1999)).

In July, 2000, the FTC indicated its support of an industry self-regulation plan to protect consumers' privacy in the area of online profiling. The industry plan was authored by the Network Advertising Initiative ("NAI"), a coalition of the country's largest profile marketers, in consultation with the FTC, which promised that NAI member marketers would not use Social Security numbers or personally identifiable sensitive medical or financial information under any circumstances.

The NAI guidelines, largely directed toward nonpersonally identifiable information, specify that each Web site will provide notice that profiling activity is occurring and that consumers will be told they can "opt out" of such information collection. Additionally, the fact that profiling activity is occurring will be revealed in any participating Web site's privacy policy.

In cases where personally identifiable information is being collected and will be merged with nonpersonally identifiable profiling information collected online (eliminating the Web user's anonymity), consumers are to be given "robust notice" and the opportunity to opt out of this form of information collection.

Lastly, the NAI guidelines address situations in which a marketer wants to link personally identifiable information with nonpersonally identifiable profile data that was collected without the consumer's prior consent. Marketers may not merge this information unless the consumer affirmatively "opts in" (consents) to this practice.

With regard to access, the NAI guidelines promise that consumers will be given "reasonable" access to personally identifiable information kept by profile marketers. This is what the FTC recommended, consistent with its position that "while access is widely recognized as an important fair information practice, the Commission believes that access presents unique implementation issues that require consideration before its parameters can be defined."

Under the NAI guidelines, network advertisers promise to make reasonable efforts to protect profiling information from loss, destruction, or improper access. Enforcement of the NAI guidelines is to be provided by industry seal program administrators such as BBB*Online* or TRUSTe.

While FTC reaction to the guidelines was largely positive, it felt that "backstop legislation" is still needed because the NAI plan does not reach non-NAI members, nor can NAI members effectively compel their members to comply. "Accordingly, the Commission

recommends legislation that would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to profiling," a commission report stated. "Such legislation would set out the basic standards of practice governing the collection and use of information online for profiling, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act, including the authority to enforce those standards."

E. Consumers

The disclosure requirements that characterize most policy and regulatory provisions assume that informed consumers can better protect themselves in a number of ways. One way is to directly influence a company's practices and policies by complaining about information practices that offend them. For example, when Intel Corp. introduced it's 1999 Pentium III chip, which contained a serial number that allowed Intel to trace equipment, it provoked an immediate public outcry, causing it to disable the numbers.[112] Microsoft Corp. experienced a similar incident when the public learned that Windows identification numbers could be used by the company to trace users. Microsoft agreed to modify the feature in response to an uproar from privacy activists.[113]

Informed consumers are also more likely to make more intelligent choices about whether to provide personal information, to buy software that blocks business' ability to collect information or to use the same technology widely used to block children's access to adult web sites to block their own access to sites which they feel offers inadequate privacy protection. Indeed, a set of computer-language protocols recently developed at the Massachusetts Institute of Technology allows consumers to set their own levels of privacy for online browsing. In a show of support, the Clinton Administration incorporated the technology ("P3P") into its White House and Commerce Department home pages and Microsoft Corp. plans to install P3P into the next version of its Windows Operating System.[114]

Finally, informed consumers influence data collection prac-

112. Krol, *supra* note 30, at 22.
113. *Id.*
114. Glenn R. Simpson, *Clinton Supports Move to Protect Consumer Privacy on the Internet*, WALL ST. J., June 22, 2000, at B14.

tices in an even more powerful way: avoiding e-commerce altogether. Only "a modest number of people accessing the Internet are actually purchasing goods or services through a Web-based transaction."[115] People are reluctant to buy online because they must watch personal information (such as a credit card number) disappear into the black hole of marketspace. When asked why they do not want to provide such information, "consumers report a fear that companies will misuse personal information."[116]

Consequently (and ironically), the very kind of regulation industry most fears may actually boost the Internet economy by reducing consumer fears. Senator Max Cleland recently said as much when he pointed out that "the 'bitter pill' of regulation could be beneficial to the health of online business: Fear is a terrible thing. Millions of people can react in fear from just one or two horror stories. We don't want to kill the goose that lays the golden eggs.[117]

Online entrepreneurs should be outdoing one another to offer consumers the most appealing privacy policies. Amazingly, they are not.

IV. THE EUROPEAN UNION

It remains to be seen which of these influences (self-regulation, legislation and consumer's choices) will most affect American online information practices, but it's quite possible that *European* privacy laws will dwarf them all. A growing share of the Internet market is occurring outside the United States. European Internet access is expected to surpass that of the United States within three years. As a result, American online businesses may soon be playing by more restrictive European privacy rules.

Imagine the tens of millions of messages containing personal data that are sent to the United States from Europe each day being cut off: no transatlantic personal banking or brokerage transactions, no airline or hotel reservations, no Internet or catalog sales, no credit checks, no European credit card purchases and no ability of corporate headquarters in the United States to manage their 9 million employees in Europe.

Such a cut-off would immediately destroy a $1.5 trillion transatlantic economic relationship. And that is what a 1998 European

115. Caudill & Murphy, *supra* note 98, at 8.
116. *Id.*
117. *Senators Mark Out Territory, Seek Support for Different Privacy Protection Proposals*, BNA No. 25, June 21, 2000, at 662.

Union ("EU") directive on personal data privacy would have done. The directive set up a comprehensive data protection regime that tried to anticipate every possible problem. It established data protection czars in every EU country to decide how much privacy each European gets.

The U.S. government considered adopting something similar in the 1970s, but decided that it could lead to government invasion of privacy. The U.S. has pointed out that the EU directive was conceived over a dozen years ago, before there was a World Wide Web. Still, the European Union insisted on applying its antiquated framework to America—the world's most sophisticated information economy.

The EU Data Privacy Directive requires marketers "to obtain unambiguous consent from a person before each use of their personal data."[118] More importantly, it requires that international transfers of personal data take place only to countries that offer an "adequate" level of personal data protection.

Because of the philosophical differences between America (which uses a mix of piecemeal legislation, regulation and self-regulation, and generally supports the consumer's right to "opt out") and the EU (which tightly restricts both the use and transfer of personal data, and the consumer's right to "opt in"), American companies feared that their information practices would not be considered "adequate," preventing them from competing in the world economy if not allowed to gather personal data from Europeans.

To avoid that, the U.S. Department of Commerce began intense negotiations with the EU. As previously discussed, the result has been the creation of Safe Harbor Programs. Under a June, 2000 agreement between the Commerce Department and the European Commission, U.S. companies will have a voluntary, self-regulatory regime, called a "safe harbor."

To be approved, a safe harbor program must adhere to the fundamental principles of notice, choice, onward transfer (limiting transfer of personal data to other parties which have safe harbor principles), security, data integrity, access and enforcement.[119] Here's how it works:

---

118. James Heckman, *A Round-up of Regulatory Proposals; Debates Should Wind Down By Year's End*, MKTG. NEWS, Aug. 30, 1999, at 4.

119. PERRITT, JR., *supra* note 28, at 40-42 (citing U.S. Department of Commerce *International Safe Harbor Privacy Principles* (Apr. 19, 1999)).

NOTICE. Businesses must tell people why they are collecting personal information and how they plan to use it, including whether they will transfer it to third parties.

CHOICE. If businesses want to use the data in another way, people must be given a chance to say no before going ahead. If the information is sensitive, such as medical data, the individual must actually say "yes" before the company may use the data differently.

THIRD PARTIES. Personal data may be sent only to third parties who have signed up for the safe harbor or have a contract with the same effect.

ACCESS. Firms must give people access to data held on them and, if it is inaccurate, allow them to correct, amend or delete it.

ENFORCEMENT. A firm must have a dispute resolution process. Typically that will be arranged through a seal program like TRUSTe or BBB*Online*, unless they are under direct government enforcement.

The safe harbor can be complex, but much more congenial to U.S. business practices than the directive would have been. It will ensure that privacy protections are applied flexibly and help e-commerce fulfill its enormous promise.

It also gives companies the certainty they need to invest and pursue business opportunities with Europe, the U.S.'s greatest market, while avoiding a lot of European red tape and assuring European consumers that their privacy will be protected–which is essential if transatlantic commerce is to prosper.

V. E-COMMERCE AND PRIVACY: WHAT LIES AHEAD

E-commerce's future depends on how privacy policy issues are resolved. It is likely that the EU agreement has set a standard. American companies will eventually be required to implement the European "opt in" model in the United States.

Meanwhile, American consumers' concerns about personal data collection and use practices are resonating through the halls of Congress. The U.S. is reaching a point in the privacy dialogue where debaters must consider the trade-off between the benefits of data collection and use and peoples' legitimate privacy expectations.

The value to business is enormous. The growth of Internet commerce is being recognized as part of a broader "marketing information revolution" that has "enabled marketers to become more

efficient in their assessment of individual customer's needs."[120] This includes the need to spend less advertising resources while getting an exponentially greater return.

The argument that information gathering is a powerful engine which has driven the growth of e-commerce, which in turn is a powerful force in America's booming economy, is being given considerable weight. The notion that an overreaction to online privacy concerns could "kill the goose that lays the golden eggs . . . or at least significantly diminish its productivity" is taking hold.[121]

Consumers are beginning to understand that they, too, benefit from online information practices: they suffer fewer direct marketing activities and intrusions as marketers improve their targeting efficiency through more useful information.[122] Both consumers and government are realizing that tailored marketing made possible by online data collection is a useful and helpful source of product and service information.[123]

Consumers benefit in various other ways, such as the availability of credit information, which allows them to perform efficient online transactions, like applying for a mortgage to purchase a home.[124] Another, largely unrecognized benefit goes to the heart of the Web's uniqueness:

> Collecting detailed information is crucial to keeping information free .... In order to provide free service, Web page operators need to be able to charge more for the advertisements on their web pages. They will not be able to set high enough rates without the added value of detailed consumer preference data and proof that Internet advertising works.[125]

It is difficult to say that consumers should be either reassured

120. Milne, *supra* note 29, at 1.

121. Krol, *supra* note 30, at 22.

122. Phelps, Nowak & Ferrell, *Privacy Concerns and Consumer Willingness to Provide Personal Information*, J. PUB. POL'Y & MKTG., Spring 2000, at 30.

123. *Id.*

124. Nan Netherton, *Consumer Advocate, Information Specialist Urge Officials to Consider Privacy Issues*, ELEC. COM. & L. REP. (June 28, 1998). These remarks were made by Fred H. Cate, a law professor at Indiana University. Professor Cate argued at the 1998 summer meeting of the National Association of Attorneys General that in the arena of online privacy regulation, "the cure could be worse than the problem." *Id.*

125. Anandashankar Mazumdar, *FTC Issues Online Privacy Report*, ELEC. COM. & L. REP. (June 21, 2000). These remarks came from Jules Polonetsky, Chief Privacy Officer for DoubleClick, Inc., an online data aggregator. *Id.*

or frightened by the online collection and use of personal information. It is likely consumers should feel some of each. How they perceive the ratio is fundamental to the future of e-commerce, because "consumers' willingness to provide personal information substantially affects the benefits they obtain."[126] Consequently, continued free Web site availability needs to be more objectively balanced against privacy concerns in the debate.

There's no doubt that Internet data collection makes privacy intrusions easier than ever, but industry maintains that such practices are not of recent origin and also occur "all the time in the offline world."[127] While this may be true, the increased sophistication of data collection has altered the way in which people perceive such practices and privacy concerns are the result of peoples' perceptions. They find little comfort from knowing that such practices predate the Internet. Whether current information practices *legally* constitute invasion of privacy is largely irrelevant from a policy perspective. Perception is reality to the perceiver, and there's no question as to how consumers' perceptions have changed.

The debate is frequently framed as the difference between *choice* and *consent.* William Safire, who advocates the *consent* point of view, recently said:

> The word choice is used by banks, hospitals and internet companies to conceal their intrusions into the personal lives of their customers. They offer us a 'choice' to tell them not to share our most intimate secrets with others .... The intruders know that most people can't be bothered to choose to 'opt out'—to take the initiative to defend themselves.[128]

Safire defines *consent* as follows: "The word *consent* is used by those opposed to the placement of "cookies." ... We want to place the burden of seeking your express, informed consent on the marketers .... Only if you affirmatively "opt in" —give your permission"—can they track your tastes and habits."

Others, like Professor Fred Cate, agree that the "opt in" approach is expensive, impractical and "intrinsically ... *more intrusive,*"[129] because it would require even more individualized treat-

126. Varney, *supra* note 20.

127. Mazumdar, *supra* note 125 (comments of Jules Polonetsky, Chief Privacy Officer of DoubleClick).

128. William Safire, *Stop Cookie-Pushers,* N.Y. TIMES, June 15, 2000, at A27.

129. Netherton, *supra* note 124 (comments of Indiana University Law Professor Fred Cate).

ment of consumers, perhaps further reducing the level of anonymity. Cate further contends the increased costs of "opt in" may detract from the substantial benefits offered by data collection and could stunt the growth of this important sector of the economy.

Privacy advocates point out that business was making the same arguments in the 1970's, when legislation was introduced to protect credit card users, and point out that those protections actually spurred the growth of the credit card market by increasing consumer confidence.[130]

Many feel that the privacy issue goes beyond a market-centered analysis and that privacy protection trumps market considerations. Professor Joel R. Reidenberg, a law professor at Fordham University, recently told a House Subcommittee: "Privacy is a political right. Typically, in a democracy, we don't sell political rights."[131]

This viewpoint is part of an attempt by privacy advocates to remove industry from the debate altogether, which will not happen. Industry will be allowed—up to a point—a continuing opportunity to police itself.

The law will soon change to reflect fundamental societal changes. The Supreme Court's interpretations of the U.S. Constitution have ingrained the notion of a right to privacy in Americans' psyche.

Online data collection remains largely unregulated, but the technological advances in information gathering, coupled with increased consumer awareness of actual and perceived abuses, have created a new political and commercial reality for e-commerce.

Will the idea of privacy for privacy's sake take hold, paving the way for sweeping reforms? Will people exchange some privacy rights for what e-commerce can offer them?

As the debate culminates, consumers will decide what they value most; what is priceless and what is for sale. Industry, on the other hand, must get a better handle on the pulse of consumers privacy. In the end, Congress will find a balance between a fundamental American liberty and America's economic future ... and the outcome is becoming quite clear.

130. Pike & Fischer, Inc., *FTC Recommends Privacy Legislation; Senators Interested in Notice Standards*, PRIVACY LAW ADVISOR, May 31, 2000.

131. Pike & Fischer, Inc., *Fordham Professor Urges Judiciary Panel to Establish Privacy as a Fundamental Right*, PRIVACY LAW ADVISOR, May 31, 2000.

***